A Decomposition Theory for Cyclotomic Modules under the Complete Point of View

Dirk Hachenberger

Institut für Mathematik, Universität Augsburg, 86159 Augsburg, Germany
E-mail: hachenberger@math.uni-augsburg.de

Communicated by E. Kleinfeld

Received May 4, 1999

In 1986, D. Blessenohl and K. Johnsen (1986, *J. Algebra* **103**, 141–159) proved that for any finite extension E/F of Galois fields there exists a *complete normal basis generator* w of E/F, which means that w *simultaneously* generates a normal basis for E over *every* intermediate field of E/F. In a recent monograph by the author (1997, "Finite Fields: Normal Bases and Completely Free Elements," Kluwer Academic, Boston) a theory is developed which allows the study of module structures of Galois fields as extensions with respect to various subfields and which led to an exploration of the structure of complete normal basis generators as well as explicit and algorithmic constructions of these objects. In the present paper we continue the development of that theory by providing various structural results: the Complete Decomposition Theorem, the Complete Product Theorem, a Theorem on Simultaneous Generators, and a Uniqueness Theorem.

Key Words: finite/Galois field; (complete) normal basis; (completely) free/normal element; cyclotomic module; complete/simultaneous generator.

1. GALOIS FIELDS UNDER THE COMPLETE POINT OF VIEW

We consider a Galois field $F = \mathrm{GF}(q)$ and work in a fixed algebraic closure $\bar{F}$ of F. For each finite field extension K over F there is a ring homomorphism of the polynomial ring $K[x]$ to the ring $\mathrm{End}_K(\bar{F})$ of K-vector space endomorphisms, mapping h to $h(\sigma_K)$, where $\sigma_K : y \to y^{|K|}$ denotes the Frobenius automorphism of $\bar{F}$ over K (and $|K|$ the cardinality of K). By defining

$$h \circ_K w := h(\sigma_K)(w) \qquad \big(h \in K[x], w \in \bar{F}\big), \tag{1.1}$$

$\bar{F}$ is equipped with the structure of a $K[x]$-module. For simplicity, a $K[x]$-submodule of $\bar{F}$, i.e., a σ_K-invariant K-subspace of $\bar{F}$, is called a *K-module*. The finite K-modules can be described easily as the subsets of $\bar{F}$ which are annihilated by a certain class of polynomials of $K[x]$ (see [Ha1, Sect. 8]): to any monic $h \in K[x]$ which is not divisible by the polynomial x there corresponds the finite K-module $M_{K,h}$ which is the kernel of the K-endomorphism $h(\sigma_K)$ on $\bar{F}$, i.e.,

$$M_{K,h} = \{v \in \bar{F} : h \circ_K v = 0\}$$

is the set of roots of the $|K|$-linearized polynomial belonging to h (see Lidl and Niederreiter [LiNi, Chap. 3, Sect. 4]). Conversely, every finite K-module is of that form.

It is a fundamental result of the theory of Galois fields that every finite K-module is cyclic, i.e., free on one generator as a K-module (see [Ha1, Sects. 3, 7, and 8]). Any $v \in \bar{F}$ satisfying $M_{K,h} = K[x] \circ_K v$ is called a *K-generator* of $M_{K,h}$. The K-generators of $M_{K,h}$ can also be described in terms of polynomials in $K[x]$. We therefore have to introduce the notion of *orders*: for $w \in \bar{F}$, the *K-order of w* is defined to be the monic polynomial $l \in K[x]$ of least degree such that $l \circ_K w = 0$; it is denoted by $\mathrm{Ord}_K(w)$.[1] Now, the minimal polynomial of $M_{K,h}$ (with respect to σ_K) is equal to h and the K-dimension of $M_{K,h}$ is equal to the degree of h. Therefore, the K-generators of $M_{K,h}$ are exactly the elements of $\bar{F}$ whose K-order is equal to h (see [Ha1, Theorem 8.4]). Moreover, the number of K-generators of $M_{K,h}$ is equal to $\phi_K(h)$, which is defined to be the number of units in $K[x]/hK[x]$.

The case where $h = x^m - 1$ (for some integer $m \geq 1$) is of particular interest: the corresponding K-module is the unique m-dimensional extension of K in $\bar{F}$, say L, and the K-generators of L are exactly those elements of L whose conjugates under the Galois group of L/K build a K-basis for L over K, i.e., a *normal basis of L/K*. A K-generator of L is therefore also called *normal in L over K* or *free in L over K*. We conclude that the cyclicity of the modules $M_{K,h}$ generalizes the classical Normal Basis Theorem, which for extensions of arbitrary Galois fields was first proved by Hensel [He] in 1888.

In the present paper we are concerned with the particular class of *cyclotomic modules* over the field F (the precise definition is given in Section 2) which includes the class of finite extensions of F. Cyclotomic modules are F-modules which usually are equipped with further module

[1] If Q is the cardinality of K, we shall also use the term *Q-order of w* and write $\mathrm{Ord}_Q(w)$. This is well-defined as for each power q^n of q there is exactly one subfield of $\bar{F}$ with cardinality q^n.

structures arising from finite extensions of F, and it is our aim to study these modules under *the complete point of view*, i.e., by considering all these structures simultaneously. To make this precise we provide the following definition.

DEFINITION 1.1. The *coefficient field* of an (arbitrary) F-module M is the set of $\zeta \in \overline{F}$ such that $\zeta M \subseteq M$.

If $M = M_{F,g}$ (with $g \in F[x]$ being monic and indivisible by x), then the coefficient field of M is in fact a finite field extension of F, which throughout is denoted by F_g. In terms of g, the coefficient field F_g is recognized as follows (see [Ha1, Sect. 11]): let $d \geq 1$ be the largest integer such that g is of the form $f(x^d)$ (for some $f \in F[x]$); then F_g is the unique d-dimensional extension of F in $\overline{F}$.

DEFINITION 1.2. Let $g \in F[x]$ be monic and indivisible by x. Then the F-dimension $\kappa(g) = \kappa_F(g) := [F_g : F]$ of F_g over F is called the *module character of* $M_{F,g}$ *over* F.

The latter terminology is motivated by the fact that for *each* intermediate field K of F_g over F (i.e., for each divisor d of $\kappa(g)$), the set $M_{F,g}$ carries the structure of a K-module. Moreover, see again [Ha1, Sect. 11], as a K-module, $M_{F,g}$ is equal to $M_{K,f(x^{[F_g:K]})}$, where f is the monic polynomial in $F[x]$ such that $g = f(x^{\kappa(g)})$. Now, recalling that for *each* K the set $M_{F,g}$ is cyclic as K-module, it is natural to ask whether there exist elements which *simultaneously* are K-generators for various K. The answer is very satisfying: for each g, the module $M = M_{F,g}$ is *completely cyclic* in the following sense (a proof of Theorem 1.3 is given in [Ha1, Sect. 12]).

THEOREM 1.3. *Let $M \subset \overline{F}$ be a finite F-module. Then there exist elements v in M such that $K[x] \circ_K v = M$ for* all *intermediate fields K of F_g over F. Each such element is therefore called a* complete generator for $M_{F,g}$ over F.

Throughout, we denote by $\Omega_F^c(g)$ the set of complete generators of $M_{F,g}$ over F, and by $\phi_F^c(g)$ the cardinality of $\Omega_F^c(g)$.

Again, the case $g = x^n - 1$ (where $n \geq 1$ is some integer) is of particular interest. Then $F_g = M_{F,g}$ and F_g is equal to the unique n-dimensional extension over F, say E. Moreover, the complete generators for E are exactly those elements which simultaneously generate a normal basis for E over *every* intermediate field K of E/F. Those elements are therefore called *completely normal in E over F* or *completely free in E over F*. For arbitrary extensions of Galois fields the existence of completely free elements was first proved by Blessenohl and Johnsen [BlJo] in 1986. We

therefore conclude that Theorem 1.3 generalizes the *Complete Normal Basis Theorem* of Blessenohl and Johnsen.[2]

In Hachenberger [Ha1] we started the development of a structure theory for completely free elements which in particular led to explicit constructions of those objects for arbitrary extensions of Galois fields.[3] In the present paper, we shall extend the structure theory of [Ha1] by providing results on complete generators for the class of *cyclotomic modules* (see Definition 2.1). An outline of the main results is given in the next section.

2. CYCLOTOMIC MODULES, AN OUTLINE

Throughout, let $F = \mathrm{GF}(q)$ and p be the characteristic of F. In contrast to the well-known function ϕ_F (the q-analogue of Euler's totient function) the complete version ϕ_F^c is extremely difficult to handle, because, by definition, its evaluation requires the study of *all* submodule-lattices of an F-module corresponding to the divisors of its module character. In general, difficulties may arise already when seeking to handle simultaneously *two* module structures (see [Ha1, Sect. 14]). For the class of cyclotomic modules we shall here prove a product formula for ϕ_F^c which translates into a decomposition of the corresponding sets of complete generators.

DEFINITION 2.1. Let $k, t \geq 1$ be integers, where k is not divisible by p, and let $g = \Phi_k(x^t)$, where $\Phi_k \in F[x]$ denotes the kth cyclotomic polynomial. Then g is called a *suitable polynomial over* F. The corresponding F-module $M_{F,g}$ is called a *cyclotomic module over* F.

Throughout we shall frequently use the basic properties of suitable polynomials from Section 10 in [Ha1]. By [Ha1, Proposition 18.2], the module character of $g = \Phi_k(x^t)$ (i.e., the module character of the corresponding F-module $M_{F,g}$) is equal to

$$\kappa\big(\Phi_k(x^t)\big) = \frac{kt}{\nu(k)}, \tag{2.1}$$

where $\nu(k)$ denotes the square-free part of k. In the present paper it is our aim to characterize an arbitrary complete generator of a cyclotomic module in terms of a decomposition of the corresponding suitable polynomial. A *decomposition* Δ *of* g *over* F is simply a set of monic pairwise

[2] The existence of completely normal elements also holds for finite Galois extensions of infinite fields (see [BlJo]). A proof of the latter fact was first given by Faith [Fa].

[3] In fact, one can derive from [Ha1] a deterministic polynomial time (in $\log|F|$ and $[E:F]$) algorithm which finds a completely free element in E/F, once an irreducible monic F-polynomial of degree $[E:F]$ is given.

relatively prime polynomials with coefficients from F such that $g = \prod_{\delta \in \Delta} \delta$, whence $M_{F,g} = \oplus_{\delta \in \Delta} M_{F,\delta}$. The decomposition Δ is called *suitable*, if each $\delta \in \Delta$ is suitable. We seek to find suitable decompositions Δ of g such that the set $\Omega_F^c(g)$ of complete generators for $M_{F,g}$ over F is decomposed as

$$\Omega_F^c(g) = \sum_{\delta \in \Delta} \Omega_F^c(\delta),$$

with the right hand side being the set of all sums $\sum_{\delta \in \Delta} w_\delta$ with $w_\delta \in \Omega_F^c(\delta)$ for each $\delta \in \Delta$. In that case one has

$$\phi_F^c(g) = \prod_{\delta \in \Delta} \phi_F^c(\delta).$$

DEFINITION 2.2. A suitable decomposition Δ of a suitable polynomial $g \in F[x]$ is called *agreeable over* F, if $\Omega_F^c(g) = \sum_{\delta \in \Delta} \Omega_F^c(\delta)$. If additionally $|\Delta| \geq 2$ then Δ is called *non-trivial*.

The main difficulty in finding non-trivial agreeable decompositions Δ lies in the fact that the module character of the component δ of Δ is a *proper* divisor of the module character of g: if $h = \Phi_l(x^s)$ is a suitable polynomial which divides $g = \Phi_k(x^t)$, then ls divides kt and there is a divisor τ of t such that $l = k\tau$. Therefore, by (2.1), $\kappa(h)$ divides $\kappa(g)$ and equality holds if and only if $\tau = 1$ and $s = t$, whence $h = g$ (see also the proof of Proposition 18.7 in [Ha1]). Consequently, the agreeability of a non-trivial decomposition Δ of g implies that complete generators for g can be recognized by considering the simpler problem of finding arbitrary complete generators for every δ in Δ, as for each such δ one needs to consider only the intermediate fields between F and F_δ where F_δ is a proper subfield of F_g.

EXAMPLE 2.3. Let $F = \mathrm{GF}(2)$. Then $\Delta = \{x - 1, \Phi_3, \Phi_9, \Phi_7(x^3), \Phi_{63}\}$ is an agreeable decomposition of $x^{63} - 1$ over F (as will be explained below, this is an application of the Complete Decomposition Theorem). The module characters of the parts are equal to 1, 1, 3, 3, and 3, respectively, while the module character of $x^{63} - 1$ is equal to 63. Therefore, the six module structures of $\mathrm{GF}(2^{63}) = M_{F,x^{63}-1}$ can effectively be handled by considering at most two module structures occurring on the components of the above agreeable decomposition Δ.

We shall now describe a procedure how agreeable decompositions can be obtained (see also [Ha1, Sect. 18]). Let therefore $g = \Phi_k(x^t)$ be as above. To each prime divisor $r \neq p$ of t which is prime to k, there is

associated a canonical decomposition of g, namely,

$$\Delta_r(g) := \{\delta_r(g), \varepsilon_r(g)\}, \tag{2.2}$$

where

$$\delta_r(g) := \Phi_k(x^{t/r}) \qquad \text{and} \qquad \varepsilon_r(g) := \Phi_{kr}(x^{t/r}). \tag{2.3}$$

By (2.1), we have

$$\kappa(\delta_r(g)) = \frac{\kappa(g)}{r} = \kappa(\epsilon_r(g)), \tag{2.4}$$

i.e., the module character of each component of $\Delta_r(g)$ is a maximal divisor of the module character of g. Since the module structure of $M_{F,g}$ with respect to fields K such that $F \subseteq K \subseteq F_{\delta_r(g)} = F_{\epsilon_r(g)} \subset F_g$ is induced by the K-module structures of $M_{F,\delta_r(g)}$ and $M_{F,\varepsilon_r(g)}$, in the decomposition $M_{F,g} = M_{F,\delta_r(g)} \oplus M_{F,\varepsilon_r(g)}$ one has

$$\Omega_F^c(g) \subseteq \Omega_F^c(\delta_r(g)) + \Omega_F^c(\epsilon_r(g)). \tag{2.5}$$

Next, let t' be the largest divisor of t which is prime to p, let R be the largest power of r dividing t, and let $\operatorname{ord}_{\nu(kt')}(q)$ be the multiplicative order of q modulo the square-free part of kt' (i.e., $\operatorname{ord}_{\nu(kt')}(q)$ is the least positive integer d such that $q^d - 1$ is divisible by $\nu(kt')$). Under the assumption that $\operatorname{ord}_{\nu(kt')}(q)$ is not divisible by R, it is proved in Section 19 of [Ha1] that $\Delta_r(g)$ (see (2.2)) is in fact an agreeable decomposition of g over F; i.e., equality holds in (2.5). Now, one of the main results of the present paper is that the latter number theoretical condition, namely that $\operatorname{ord}_{\nu(kt')}(q)$ *is not divisible by* R, is also *necessary* for $\Delta_r(g)$ to be agreeable over F (the latter was conjectured in [Ha1, p. 113]). Summarizing, we have the following structure theorem on complete generators for cyclotomic modules (which extends the Decomposition Theorem of [Ha1, p. 111]).

COMPLETE DECOMPOSITION THEOREM (CDT). *Let $g = \Phi_k(x^t)$ be a suitable polynomial over $F = \mathrm{GF}(q)$, let $r \neq p$ be a divisor of t which does not divide k, and let R be the largest power of r dividing t. Moreover, let t' be the largest divisor of t which is prime to p. Then $\Delta_r(g)$ is agreeable over F if and only if $\operatorname{ord}_{\nu(kt')}(q)$ is not divisible by R.*

EXAMPLE 2.3 (Continued). We demonstrate that $\Delta = \{x - 1, \Phi_3, \Phi_9, \Phi_7(x^3), \Phi_{63}\}$ is an agreeable decomposition of $x^{63} - 1$ over $F = \mathrm{GF}(2)$. Starting with $g = x^{63} - 1$ and $r = 7$, (CDT) implies that $\{x^9 - 1, \Phi_7(x^9)\}$ is agreeable over F. Next, apply (CDT) to $x^9 - 1$ with $r = 3$ to obtain that $\{x^3 - 1, \Phi_9\}$ is agreeable over F. We may also apply (CDT) to $\Phi_7(x^9)$ with

$r = 3$ and see that $\{\Phi_7(x^3), \Phi_{63}\}$ is agreeable over F. Finally, (CDT) can be applied once more (to $x^3 - 1$ again with $r = 3$) to obtain that $\{x - 1, \Phi_3\}$ is agreeable. All together, this proves the agreeability of Δ. Observe that (CDT) cannot be applied to $\Phi_7(x^3)$ with $r = 3$ as $\mathrm{ord}_{21}(2) = 6$ is divisible by 3.

Of course, the proof of the necessity of the number theoretical condition in (CDT) (once more, that $\mathrm{ord}_{\nu(kt')}(q)$ is not divisible by R) is far from being trivial, as, by contradiction, under the assumption that R divides $\mathrm{ord}_{\nu(kt')}(q)$, we have to determine complete generators for $M_{\cdot, \delta_r(g)}$ and $M_{F, \epsilon_r(g)}$, respectively, whose sum behaves badly in the sense that it does *not* give a complete generator for $M_{F,g}$. The proof of that part of (CDT) can only be finished in Section 5 of the present paper. It will require two preliminary results which are also of individual interest.

For the first tool, the *Complete Product Theorem*, we have to introduce a binary operation on certain suitable polynomials.[4] Assume that $m, n, s, t \geq 1$ are integers such that ms and nt are relatively prime, and such that nm is not divisible by p. Then

$$\Phi_m(x^s) * \Phi_n(x^t) := \Phi_{mn}(x^{st}). \tag{2.6}$$

COMPLETE PRODUCT THEOREM (CPT). *As above, let ms and nt be relatively prime and nm be indivisible by p. Let* $\alpha = \Phi_m(x^s)$ *and* $\beta = \Phi_n(x^t)$ *and assume that* $u \in M_{F,\alpha}$ *and* $v \in M_{F,\beta}$. *Then the following assertions are equivalent.*

(1) $u \in \Omega_F^c(\alpha)$ *and* $v \in \Omega_F^c(\beta)$,

(2) $uv \in \Omega_F^c(\alpha * \beta)$.

The implication (1) $\Rightarrow$ (2) of (CPT) is already proved in Section 25 of [Ha1]. By (2.1) we have

$$\kappa(\alpha * \beta) = \kappa(\alpha)\kappa(\beta), \tag{2.7}$$

whence (1) $\Rightarrow$ (2) provides an important tool for determining complete generators (see [Ha1, Chap. VI] for more details). In Section 3 of the present paper we shall prove the implication (2) $\Rightarrow$ (1).

EXAMPLE 2.3 (Continued). We consider again the extension $E = \mathrm{GF}(2^{63})$ over $F = \mathrm{GF}(2)$. Let η be any primitive 27th root of unity, let ξ be a root of $x^7 + x^3 + 1$, and ζ a root of $x^7 + x + 1$ (both polynomials are irreducible over F). Then, using results of Chapter VI of [Ha1], it holds

[4] In order to avoid confusion with the scalar multiplication defined in (1.1), instead of $\circ$ in [Ha1], we here prefer the notation $*$.

that

$$u := \eta^3 + \eta^6 + \eta^{-3} + \eta^{-6} \in \Omega_F^c(\Phi_3),$$
$$v := \eta + \eta^2 + \eta^{-1} + \eta^{-2} \in \Omega_F^c(\Phi_9),$$
$$w := \xi + \zeta \in \Omega_F^c(\Phi_7).$$

An application of (CDT) shows that $1 + u \in \Omega_F^c(\Phi_1(x^3))$ and applications of (CPT) show that $w(1 + u) \in \Omega_F^c(\Phi_7(x^3))$ and that $wv \in \Omega_F^c(\Phi_{63})$. Thus, by the agreeability of the decomposition Δ of $x^{63} - 1$ given above, we have that $1 + u + v + w(1 + u) + wv$ is completely free in E over F.

The second tool which is necessary to complete the proof of (CDT) is the *Theorem on Simultaneous Generators* (TSG), a technical result which is postponed to Section 4.

In Section 6, which is the last part of the present paper, we shall further discuss our *decomposition model* which is based on the class of cyclotomic modules and (CDT). Recall that in Example 2.3, we have obtained the agreeable decomposition $\Delta = \{x - 1, \Phi_3, \Phi_9, \Phi_7(x^3), \Phi_{63}\}$ of $x^{63} - 1$ over GF(2) by applying (CDT) several times, and we have mentioned that Δ cannot be refined by a further application of (CDT). In Section 6, we will prove that, for any suitable polynomial, a recursive application of (CDT) results in a *unique* agreeable decomposition to which (CDT) cannot be applied anymore, no matter in which order the various primes r have been chosen in the course of applying (CDT) (the validity of the latter result is mentioned in [Ha1, p. 113], but a proof is not given there). In summary, we can say that, under the complete point of view, (CDT) provides a tool which produces a unique agreeable decomposition into components which, within our model, are *irreducible*.

We finally shall remark that for general suitable polynomials g there are suitable decompositions which are *not* obtained through a recursive application of (CDT). For example,

$$\Delta = \{\Phi_{31}, \Phi_{5\cdot 31}(x^3), \Phi_{3\cdot 31}(x^2), \Phi_{2\cdot 31}(x^5), \Phi_{30\cdot 31}\} \tag{2.8}$$

is such a decomposition of $g = \Phi_{31}(x^{30})$: one easily checks that for each prime divisor r of $t = 30$ there exists a $h_r \in \Delta$ such that $\gcd(h_r, \delta_r(g)) \neq 1$ and $\gcd(h_r, \varepsilon_r(g)) \neq 1$.

3. THE COMPLETE PRODUCT THEOREM

In the present section we will prove the Complete Product Theorem (CPT). As mentioned in Section 2, the implication (1) $\Rightarrow$ (2) is already

shown in [Ha1, Sect. 25], whence we concentrate on the proof of the implication (2) $\Rightarrow$ (1). The latter is essentially based on the following proposition.

PROPOSITION 3.1. *Let $m, n, s, t \geq 1$ be integers such that the characteristic p of F does not divide mn and assume that ms and nt are relatively prime. Let $\alpha = \Phi_m(x^s)$ and $\beta = \Phi_n(x^t)$ and assume that $u \in M_{F,\alpha}$ and $v \in M_{F,\beta}$. Then the following assertions are equivalent.*

(i) $\mathrm{Ord}_F(u) = \alpha$ *and* $\mathrm{Ord}_F(v) = \beta$,

(ii) $\mathrm{Ord}_F(uv) = \alpha * \beta = \Phi_{mn}(x^{st})$.

Proof. Again, the implication (i) $\Rightarrow$ (ii) is provided in Section 25 of [Ha1], whence we restrict our attention to the part (ii) $\Rightarrow$ (i). Assume therefore that $\mathrm{Ord}_F(uv) = \alpha * \beta$, where $u \in M_{F,\alpha}$ and $v \in M_{F,\beta}$.

Since ms and nt are relatively prime, there are integers i and j such that

$$ims \equiv 1 \bmod nt \qquad \text{and} \qquad jnt \equiv 1 \bmod ms.$$

With $\alpha = \Phi_m(x^s)$ the module $M_{F,\alpha}$ is contained in the ms-dimensional extension of F whence $\sigma_F^{ms}(y) = y$ for all $y \in M_{F,\alpha}$ and therefore

$$\sigma_F^{jnt}(y) = \sigma_F(y) \qquad \text{for all } y \in M_{F,\alpha}. \tag{3.1}$$

Analogously, with $\beta = \Phi_n(x^t)$ the module $M_{F,\beta}$ is contained in the nt-dimensional extension of F whence $\sigma_F^{nt}(y) = y$ for all $y \in M_{F,\beta}$ and therefore

$$\sigma_F^{ims}(y) = \sigma_F(y) \qquad \text{for all } y \in M_{F,\beta}. \tag{3.2}$$

Now, take elements $u_0 \in M_{F,\alpha}$ and $v_0 \in M_{F,\beta}$ such that $\mathrm{Ord}_F(u_0) = \alpha$ and $\mathrm{Ord}_F(v_0) = \beta$. Then there exist polynomials λ and μ in $F[x]$ such that $u = \lambda \circ_F u_0$ and $v = \mu \circ_F v_0$ (see (1.1) for the definition of the operator $\circ_F$). Using (3.1) and (3.2) we obtain

$$uv = (\lambda \circ_F u_0)(\mu \circ_F v_0) = \big(\lambda(x^{jnt}) \circ_F u_0\big)\big(\mu(x^{ims}) \circ_F v_0\big),$$

and once more with (3.1) and (3.2), one can show that

$$uv = \big(\lambda(x^{jnt})\mu(x^{ims})\big) \circ_F (u_0 v_0).$$

Now, by the validity of the implication (i) $\Rightarrow$ (ii) we have $\mathrm{Ord}_F(u_0 v_0) = \alpha * \beta$, while by assumption $\mathrm{Ord}_F(uv) = \alpha * \beta$. We therefore conclude that the polynomials $\lambda(x^{jnt})\mu(x^{ims})$ and $\alpha * \beta = \Phi_{mn}(x^{st})$ are relatively prime. In order to prove (ii) $\Rightarrow$ (i), we assume by contradiction that λ and

$\alpha = \Phi_m(x^s)$ or μ and β have a common root and show then that $\lambda(x^{jnt})\mu(x^{ims})$ and $\alpha * \beta$ also must have a root in common. It suffices to assume that $\gcd(\lambda, \alpha) \neq 1$, the case $\gcd(\mu, \beta) \neq 1$ being similar.

Given that $\gcd(\lambda, \alpha) \neq 1$ there exists an element $\zeta \in \bar{F}$ such that $\lambda(\zeta) = 0$ and ζ^s is a primitive mth root of unity. We show that there is an element $\eta \in \bar{F}$ such that $\lambda(\eta^{jnt}) = 0$ and η^{st} is a primitive mnth root of unity, whence η is a root of $\Phi_{mn}(x^{st}) = \alpha * \beta$. Take therefore an element $\nu \in \bar{F}$ with $\nu^{jnt} = \zeta$, whence $(\nu^{st})^{jn} = \zeta^s$ is a primitive mth root of unity and the multiplicative order of ν^{st} is of the form md where d divides nj and d is indivisible by the characteristic p of F. Next, let U be the multiplicative group of all elements ξ in $\bar{F}$ such that $\xi^{jnt} = 1$. Then $U^{st} = \{y^{st} \mid u \in U\}$ contains all roots of unity of multiplicative order dividing $jnt/\gcd(jnt, st) = nj$. Thus, taking $\xi \in U$ such that $(\xi\nu)^{st} = \xi^{st}\nu^{st}$ is a primitive mnth root of unity yields that $\eta = \xi\nu$ is a common root of $\alpha * \beta$ and $\lambda(x^{jnt})$ (and therefore also of $\lambda(x^{jnt})\mu(x^{ims})$), whence everything is proved. ∎

We are now able to settle the implication (2) ⇒ (1) of (CPT): let again $\alpha = \Phi_m(x^s)$ and $\beta = \Phi_n(x^t)$, let $u \in M_{F,\alpha}$ and $v \in M_{F,\beta}$, and assume that uv is a complete generator for $M_{F,\alpha*\beta}$. Recall from (2.7) that the module character $\kappa := \kappa(\alpha * \beta)$ of $M_{F,\alpha*\beta}$ is equal to $\kappa(\alpha)\kappa(\beta)$. Let a be a divisor of $\kappa(\alpha)$ and let K be the a-dimensional extension of F. By the assumption on uv, the K-order of uv is equal to

$$\Phi_{\nu(mn)}(x^{\kappa/a}) = \bar{\alpha} * \beta,$$

where

$$\bar{\alpha} := \Phi_{\nu(m)}(x^{\kappa(\alpha)/a}).$$

Since a is relatively prime to nt, the polynomial β is a divisor of $\Phi_n(x^{at}) = \beta(x^a)$ and therefore $\beta(\sigma_F^a)(v) = 0$ whence $v \in M_{K,\beta}$. Since further $u \in M_{K,\bar{\alpha}}$, an application of Proposition 3.1 (to K, $\bar{\alpha}$ and β) shows that u has K-order (i.e., q^a-order) equal to $\bar{\alpha}$ (and v has K-order β). Since this holds for all divisors a of $\kappa(\alpha)$, the element u is a complete generator for $M_{F,\alpha}$. By a similar reasoning one shows that v is a complete generator for $M_{F,\beta}$, and therefore (CPT) is proved. ∎

4. A THEOREM ON SIMULTANEOUS GENERATORS

In the present section we provide the second important tool for the proof of the Complete Decomposition Theorem. We therefore have to

introduce a generalization of the notion of a complete generator. Let g be a suitable polynomial over $F = \mathrm{GF}(q)$ and let N and L be subfields of the coefficient field F_g of $M_{F,g}$ such that $F \subseteq N \subseteq L$ (see Definition 1.1 and the discussion thereafter). Then $w \in M_{F,g}$ is called an *$[L/N]$-generator of $M_{F,g}$*, if w simultaneously is a K-generator for $M_{F,g}$ for every intermediate field K of L/N.

THEOREM ON SIMULTANEOUS GENERATORS (TSG). *Let $g = \Phi_k(x^t)$, where $k > 1$ is not divisible by p. Let $r \neq p$ be a prime divisor of t which does not divide k, and let R be the maximal power of r dividing t. Finally, let L be the subfield of F_g having degree t over F and let K be the subfield of F_g having degree t/r over F.*

Assume that $\mathrm{ord}_k(q)$ is divisible by t.

Then there exist $[K/F]$-generators w_δ and w_ϵ of $M_{F,\delta_r(g)}$ and $M_{F,\epsilon_r(g)}$, respectively, such that $w := w_\delta + w_\epsilon$ has not L-order Φ_k and therefore is not an $[L/F]$-generator of $M_{F,g}$.

Proof. Let f be an irreducible F-divisor of Φ_k and h an irreducible L-divisor of f. We first concentrate on the subspace $M = M_{L,f} = M_{F,f(x^t)}$ of $M_{F,g}$ which is an N-module for each intermediate field N of L/F. For each such N, let g_N be the irreducible N-divisor of Φ_k which is divisible by h and which divides f. Then, recalling the notation from Section 1, the assumption that $\mathrm{ord}_k(q)$ is divisible by t implies

$$g_N = \prod_{j=0}^{[E:N]-1} \sigma_N^j(g_E)$$

whenever N and E are fields such that $F \subseteq N \subseteq E \subseteq L$. Moreover, if $v_f \in M$ has L-order $h = g_L$, then (by an application of [Ha2, Theorem 2.2]) for all intermediate fields N of L/F, the N-order of v_f is equal to $g_N(x^{[L:N]})$ (the assumption on $\mathrm{ord}_k(q)$ is crucial for the latter, because this indicates that L is contained in the splitting field of Φ_k over F). Now, as in the assertion of the theorem, let K be the maximal subfield of index r in L and define

$$w_f := \sum_{j=0}^{[K:F]-1} \sigma_F^j(v_f). \tag{4.1}$$

We claim that for every intermediate field N of K/F, the N-order of w_f is equal to $f(x^{[L:N]})$, i.e., that w_f is a $[K/F]$-generator of M. In order to

prove the claim, observe first that

$$w_f = \sum_{i=0}^{[N:F]-1} \sum_{j=0}^{[K:N]-1} \sigma_F^{j[N:F]+i}(v_f)$$

$$= \sum_{i=0}^{[N:F]-1} \sigma_F^i \left(\sum_{j=0}^{[K:N]-1} \sigma_N^j(v_f) \right).$$

As $k > 1$, for each intermediate field N of K over F, the polynomials $(x^{[K:N]} - 1)/(x - 1)$ and $g_N(x^{[L:N]})$ are relatively prime (the latter one is the N-order of v_f). Thus, Lemma 7.4 in [Ha1] implies that $\sum_{j=0}^{[K:N]-1} \sigma_N^j(v_f)$ likewise has N-order $g_N(x^{[L:N]})$. Now, for different $i, i' \in \{0, 1, \ldots, [N:F] - 1\}$ the polynomials $\sigma_F^i(g_N(x^{[L:N]}))$ and $\sigma_F^{i'}(g_N(x^{[L:N]}))$ are relatively prime. Therefore (see once more Theorem 8.6 in [Ha1]), the N-order of w_f is equal to

$$\prod_{i=0}^{[N:F]-1} \sigma_F^i\left(g_N(x^{[L:N]})\right) = g_F(x^{[L:N]}) = f(x^{[L:N]}),$$

and this proves the claim.

However, by (4.1) and the assumption that v_f has L-order equal to h, it holds that the L-order of w_f is equal to $\prod_{i=0}^{[K:F]-1} \sigma_F^i(h)$. The latter polynomial is a *proper* divisor of f, whence w_f is *not* an L-generator of M, and hence no $[L/F]$-generator.

Next, we repeat this construction for all F-divisors f of Φ_k, and let $w := \sum_f w_f$. Using Theorem 12.2 of [Ha1], we obtain that w is a $[K/F]$-generator of M, but not an $[L/F]$-generator, as the L-order of w is not equal to Φ_k. We finally decompose M into $M_{F,\delta_r(g)} \oplus M_{F,\epsilon_r(g)}$ and consider the corresponding decomposition $w_\delta + w_\epsilon$ of w. By construction, using again Theorem 12.2 in [Ha1], we have that w_δ is a $[K/F]$-generator of $M_{F,\delta_r(g)}$ and w_ϵ is a $[K/F]$-generator of $M_{F,\epsilon_r(g)}$. This completes the proof of the theorem. ∎

5. THE COMPLETE DECOMPOSITION THEOREM

We are now prepared to finish the proof of the Complete Decomposition Theorem (CDT) by establishing its *necessary part*, i.e., by proving that the number theoretical condition "$\mathrm{ord}_{\nu(kl')}(q)$ is not divisible by R" is necessary for the decomposition $\Delta_r(g)$ to be agreeable.[5] Recall that the

[5] Throughout, we use the notation as in the assertion of (CDT). In particular, $g = \Phi_k(x^l)$ is a suitable polynomial and p is the characteristic of the underlying field $F = \mathrm{GF}(q)$.

sufficient part of (CDT), i.e., the sufficiency of "$\mathrm{ord}_{\nu(kt')}(q)$ is not divisible by R" for $\Delta_r(g)$ to be agreeable, was already proved in [Ha1, Sect. 19]. In fact, during the subsequent proof of the necessary part we shall apply the sufficient part of (CDT) in various situations. We proceed in several steps.

Step 1. Reduction to the case where t is not divisible by p. Let $t = \tau\pi$ where τ is not divisible by p, whereas π is a power of p. Let $\lambda = \Phi_k(x^\tau)$. We show that if $\Delta_r(\lambda)$ is not agreeable, then $\Delta_r(g)$ is not agreeable. Observe first that $g = \lambda * (x^\pi - 1)$ (see (2.6)). Let

$$\alpha = \delta_r(\lambda) = \Phi_k(x^{\tau/r}) \qquad \text{and} \qquad \beta = \varepsilon_r(\lambda) = \Phi_{kR}(x^{\tau/R}),$$

and assume that $\Delta_r(\lambda) = \{\alpha, \beta\}$ is not agreeable over $F = \mathrm{GF}(q)$. Then there exist elements $u_\alpha \in \Omega_F^c(\alpha)$ and $u_\beta \in \Omega_F^c(\beta)$ such that $u = u_\alpha + u_\beta$ is not a complete generator of $M_{F,\lambda}$ over F. Let $v \in \Omega_F^c(x^\pi - 1)$; then, according to the Complete Product Theorem (CPT), $w_\delta := u_\alpha v \in \Omega_F^c(\delta_r(g))$ and $w_\epsilon := u_\beta v \in \Omega_F^c(\varepsilon_r(g))$. If $w := w_\delta + w_\epsilon$ would be a complete generator of $M_{F,g}$ over F, then, again by (CPT), u would be a complete generator of $M_{F,\lambda}$ over F. This however contradicts the assumption and finishes the analysis of Step 1.

From now on we assume that t is not divisible by p. Since R divides $\mathrm{ord}_{\nu(kt)}(q)$ and R is the power of a prime, it is clear that R divides $\mathrm{ord}_s(q)$ for some prime divisor $s \neq r$ of kt. We have to distinguish the cases where s divides k and s divides t, respectively.

Step 2. Assume that s divides t. Let S be the largest power of s dividing t and write $t = \tau RS$. Then $g = \rho * \mu$ where $\rho := x^{SR} - 1$ and $\mu := \Phi_k(x^\tau)$.

Step 2a. Reduction to the case where $g = \rho$. We show that if $\Delta_r(\rho)$ is not agreeable, then $\Delta_r(g)$ is not agreeable.

Let $\alpha := x^{SR/r} - 1$ and $\beta := \Phi_R(x^S)$ and assume that $\Delta_r(\rho) = \{\alpha, \beta\}$ is not agreeable over F. Choose $u_\alpha \in \Omega_F^c(\alpha)$ and $u_\beta \in \Omega_F^c(\beta)$ such that $u := u_\alpha + u_\beta$ is not a complete generator of $M_{F,\rho}$ over F, and let $v \in \Omega_F^c(\mu)$. Then $w_\delta := u_\alpha v$ is a complete generator of $M_{F,\delta_r(g)}$ over F and $w_\epsilon := u_\beta v$ is a complete generator of $M_{F,\epsilon_r(g)}$ over F, for otherwise u would be a complete generator of $M_{F,\rho}$ over F, which contradicts the assumption.

Step 2b. Proof of the assertion for $g = \rho$. We proceed via induction on the exponent of s in S. Assume first that $s = S$. Let

$$\alpha := x^{R/r} - 1 \qquad \text{and} \qquad \beta := \Phi_R \quad \text{and} \quad \gamma := \Phi_s(x^R).$$

Applying the sufficient part of (CDT) twice shows that $\{\alpha, \beta, \gamma\}$ is agreeable over F. However, by (TSG) in Section 4, which yields an assertion on

complete generators in the current situation, $\Delta_r(\gamma)$ is not agreeable for γ over F, since there exist complete generators y of $M_{F,\delta_r(\gamma)}$ over F and z of $M_{F,\epsilon_r(\gamma)}$ over F such that $y+z$ does not have q^R-order Φ_s. Now, let $a \in \Omega_F^c(\alpha)$ and $b \in \Omega_F^c(\beta)$. The q^R-order of $a+b+y+z$ is not equal to $x^s - 1$. But, as

$$\alpha\delta_r(\gamma) = (x^{R/r} - 1) \cdot \Phi_s(x^{R/r})$$

gives an agreeable decomposition of $x^{sR/r} - 1$ (by the sufficient part of (CDT)), it holds that $a + y \in \Omega_F^c(x^{sR/r} - 1)$. Similarly,

$$\beta\varepsilon_r(\gamma) = \Phi_R \cdot \Phi_s(x^R)$$

is an agreeable decomposition of $\Phi_R(x^s)$ over F, whence $b + z \in \Omega_F^c(\Phi_R(x^s))$. We therefore conclude that $(x^{SR/r} - 1) \cdot \Phi_R(x^s)$ is not agreeable for $x^{sR} - 1$ over F.

We assume next that S is divisible by s^2. Let

$$\alpha := x^{R/r \cdot S/s} - 1 \qquad \text{and} \qquad \beta := \Phi_R(x^{S/s}),$$

and

$$\eta := \Phi_S(x^{R/r}) \qquad \text{and} \qquad \zeta := \Phi_{SR}.$$

By induction, $\{\alpha, \beta\}$ is not agreeable over F. Thus, there exist complete generators a and b over F for the F-modules corresponding to α and β, respectively, such that $a + b$ is not a complete generator for the F-module corresponding to $x^{RS/s} - 1$. Let $x + y$ be the decomposition of a complete generator for $M_{F,\Phi_S(x^R)}$ according to the decomposition $\{\eta, \zeta\} = \Delta_r(\Phi_S(x^R))$. Now, as $\{\alpha, \eta\}$ is agreeable over F (this is an application of the sufficient part of (CDT) to $\delta = x^{SR/r} - 1$ with s as prime), $a + x$ is a complete generator for $M_{F,\delta}$ over F. Similarly, $\{\beta, \zeta\}$ is agreeable over F, whence $b + z$ is a complete generator for $M_{F,\varepsilon}$ over F, where $\varepsilon = \Phi_R(x^S)$. By construction, however, $a + b + x + y$ is not a complete generator for g over F. This finishes Step 2b and Step 2.

Step 3. Assume that s divides k. Let S be the largest power of s dividing k and write $k = \kappa S$. Let $t = \tau R$, $\rho := \Phi_S(x^R)$, and $\mu := \Phi_\kappa(x^\tau)$. Then $\rho * \mu = g$. Again, we break up the analysis into two further steps.

Step 3a. Reduction to the case where $g = \rho$. We show that if $\Delta_r(\rho)$ is not agreeable, then $\Delta_r(g)$ is not agreeable.

Let $\alpha = \Phi_S(x^{R/r})$ and $\beta = \Phi_{SR}$. Assume that $u_\alpha \in \Omega_F^c(\alpha)$ and $u_\beta \in \Omega_F^c(\beta)$, whereas $u = u_\alpha + u_\beta$ is not a complete generator for $M_{F,\rho}$ over F. If $v \in \Omega_F^c(\mu)$, then $w_\delta := u_\alpha v$ and $w_\varepsilon := u_\beta v$ are complete generators for the F-modules corresponding to $\alpha * \mu = \delta$ and $\beta * \mu = \varepsilon$, respectively. However, an application of (CPT) shows that $w = w_\delta + w_\varepsilon$ is not a complete generator of $M_{F,g}$ over F.

Step 3b. Assume that $g = \rho$. Observe first that s is different from 2, as R divides $e := \mathrm{ord}_s(q)$. Further, the multiplicative order of q modulo S is of the form es^a, where s^a divides S/s. Let $\sigma := s^{\lfloor a/2 \rfloor}$. An application of Lemma 20.4 in [Ha1] shows that $\mathrm{ord}_{S/\sigma}(q)$ is divisible by $R\sigma$. Let L and K be the subfields of F_g with degrees $R\sigma$ and $\sigma R/r$ over F, respectively. Viewing g as $\Phi_{S/\sigma}(x^{R\sigma})$, an application of (TSG) in Section 4 shows that there exist $[K/F]$-generators w_δ and w_ε for the F-modules corresponding to $\delta := \Phi_S(x^{R/r})$ and $\varepsilon := \Phi_{SR}$, respectively, such that $w = w_\delta + w_\varepsilon$ does not have $q^{R\sigma}$-order $\Phi_{S/\sigma}$, and therefore is not an $[L/F]$-generator of $M_{F,g}$. We claim that w_δ and w_ε even are complete generators of $M_{F,\delta}$ and $M_{F,\varepsilon}$, respectively, and this finishes the analysis of Step 3.

In order to prove the claim, it remains to show that for each divisor d of R/r and each divisor $b \neq 1$ of $S/(s\sigma)$ the $q^{\sigma bd}$-order of w_δ is equal to $\Phi_{S/(\sigma b)}(x^{R/(rd)})$ and the $q^{\sigma bd}$-order of w_ε is equal to $\Phi_{(SR)/(\sigma bd)}$. We know that the $q^{\sigma d}$-order of w_ε is equal to $\Phi_{(SR)/(\sigma d)}$. Since s does not divide the multiplicative order of q modulo $(SR)/(\sigma bd)$ (this relies on the choice of σ) the desired result for w_ε follows as an application of Lemma 15.3 of [Ha1]. Similarly, the $q^{\sigma d}$-order of w_δ is equal to the polynomial $\Phi_{S/\sigma}(x^{R/(dr)})$, which decomposes as $\Pi_{e|R/(dr)}\Phi_{eS/\sigma}$. According to this decomposition, we split up w_δ as $\Sigma_e w_e$, the eth component having $q^{\sigma d}$-order $\Phi_{eS/\sigma}$. Now, an application of Lemma 15.3 of [Ha1] to each component of that decomposition in combination with Theorem 8.6 of [Ha1] yields the desired result for w_δ. This all together finishes the proof of (the necessary part of) the Complete Decomposition Theorem. ∎

6. THE DECOMPOSITION MODEL, A DISCUSSION

In this final section we study some properties of our decomposition model which is based on the Complete Decomposition Theorem (DCT) and the class of cyclotomic modules.

We have already argued after Definition 2.2 that if $h = \Phi_l(x^s)$ is a suitable polynomial dividing $g = \Phi_k(x^t)$, then ls divides kt and there is a divisor τ of t such that $l = k\tau$. Using this (and properties of suitable polynomials from Section 10 of [Ha1]) one can show that if h is a *maximal*

suitable divisor of g (which of course means that there exists no suitable polynomial f different from h and g which divides g and which is divisible by h), then there exists a prime divisor r of t which does not divide k such that one of the following cases occurs:

(1) $r = p$ is the characteristic of F and $h = \Phi_k(x^{t/r})$, i.e., $h^p = g$;

(2) r is distinct from p and $h = \delta_r(g)$ or $h = \varepsilon_r(g)$.

The latter remotivates our approach in Section 2.

Now, given a suitable polynomial g over F, we shall show that there is obtained a unique (finest) agreeable decomposition of g by a recursive application of (CDT) (as indicated in Example 2.3), no matter in which order the various primes r have been chosen in the course of applying (CDT). For this purpose, we define the *agreeable decomposition tree* $\Gamma(g)$ over F as follows: the first layer Γ_1 consists of the single set $\{g\}$; given the ith layer Γ_i ($i \geq 1$), the $(i+1)$st layer consists exactly of those sets H for which there exists a set C in Γ, a suitable polynomial $c = \Phi_l(x^s) \in C$, and a prime divisor $r \neq p$ of s such that $H = (C \setminus \{c\}) \cup \Delta_r(c)$, where $\Delta_r(c)$ is agreeable for c over F (the latter property can efficiently be checked with (CDT)). Moreover, C and H are connected by a directed arc $C \to H$.

UNIQUENESS THEOREM (UT). *Given a suitable polynomial g over F, then the agreeable decomposition tree $\Gamma(g)$ over F has a unique sink, i.e., the layer with highest index consists of a single set Z, which is the unique set in $\Gamma(g)$ from which no arc leaves. Moreover, for every arc $C \to H$ in $\Gamma(g)$ there exists a path from C to Z which starts in $C \to H$.*

Proof. We may assume that k and t are relatively prime (see [Ha1, Sect. 10]). The assertion of the theorem is true if t has only one prime divisor r which is different from p, since in that case, $\Gamma(g)$ consists of a path. The general assertion is proved by induction on the number of distinct prime divisors $r \neq p$ of t counted with multiplicity. Assume therefore that $\Gamma(g)$ has two different sinks X and Y. Choose two paths from $\{g\}$ to X and Y, respectively, starting with the arcs $\{g\} \to \Delta_r(g)$ and $\{g\} \to \Delta_s(g)$, respectively, where r and s are prime divisors of t, different from p. By induction, X is the union of the unique sinks of $\Gamma(\delta_r(g))$ and $\Gamma(\varepsilon_r(g))$, while Y is the union of the two unique sinks of $\Gamma(\delta_s(g))$ and $\Gamma(\varepsilon_s(g))$. Of course, $r \neq s$ for otherwise $X = Y$. Thus, the decompositions $\Delta_s(\delta_r(g))$, $\Delta_s(\varepsilon_r(g))$, $\Delta_r(\delta_s(g))$, and $\Delta_r(\varepsilon_s(g))$ entirely are agreeable over F, and these sets give rise to the sets $\Sigma = \Delta_s(\delta_r(g)) \cup \Delta_s(\varepsilon_r(g))$ and $\Theta = \Delta_r(\delta_s(g)) \cup \Delta_r(\varepsilon_s(g))$ in the layer Γ_4 of $\Gamma(g)$. The crucial point is that $\Sigma = \Theta$, which follows easily from (2.2) and (2.3). Therefore, by using a path through Σ and by applying the induction hypothesis to each of the four members of Σ shows that $X = Y$. Because of this contradiction, everything is proved. ∎

We have already mentioned at the end of Section 2 that for general suitable polynomials g there are suitable decompositions which do *not* occur in the agreeable decomposition tree of g (as defined above). However, in view of the efficiency of the presented results, our model seems to be the most natural one. It is certainly hopeless to try to characterize the set of complete generators of cyclotomic modules in terms of a decomposition as for instance in (2.8).

ACKNOWLEDGMENT

The author thanks the referee for many valuable remarks and in particular for providing him with the current proof of Proposition 3.1 which is more transparent than the previous one.

REFERENCES

[BlJo] D. Blessenohl and K. Johnsen, Eine Verschärfung des Satzes von der Normalbasis, *J. Algebra* **103** (1986), 141–159.

[Fa] C. C. Faith, Extensions of normal bases and completely basic fields, *Trans. Amer. Math. Soc.* **85** (1957), 406–427.

[Ha1] D. Hachenberger, "Finite Fields: Normal Bases and Completely Free Elements," Kluwer Academic, Boston, 1997.

[Ha2] D. Hachenberger, Universal normal bases for the abelian closure of the field of rational numbers, *Acta Arith* **93**, No. 4 (2000), 329–341.

[He] K. Hensel, Über die Darstellungen der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor, *J. Reine Angew. Math.* **103** (1888), 230–237.

[LiNi] R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, Reading, MA, 1983.